Usability Testing a Malware-Resistant Input Mechanism

Alana Libonati[1] Jonathan M. McCune[2] Michael K. Reiter[1]

University of North Carolina[1]

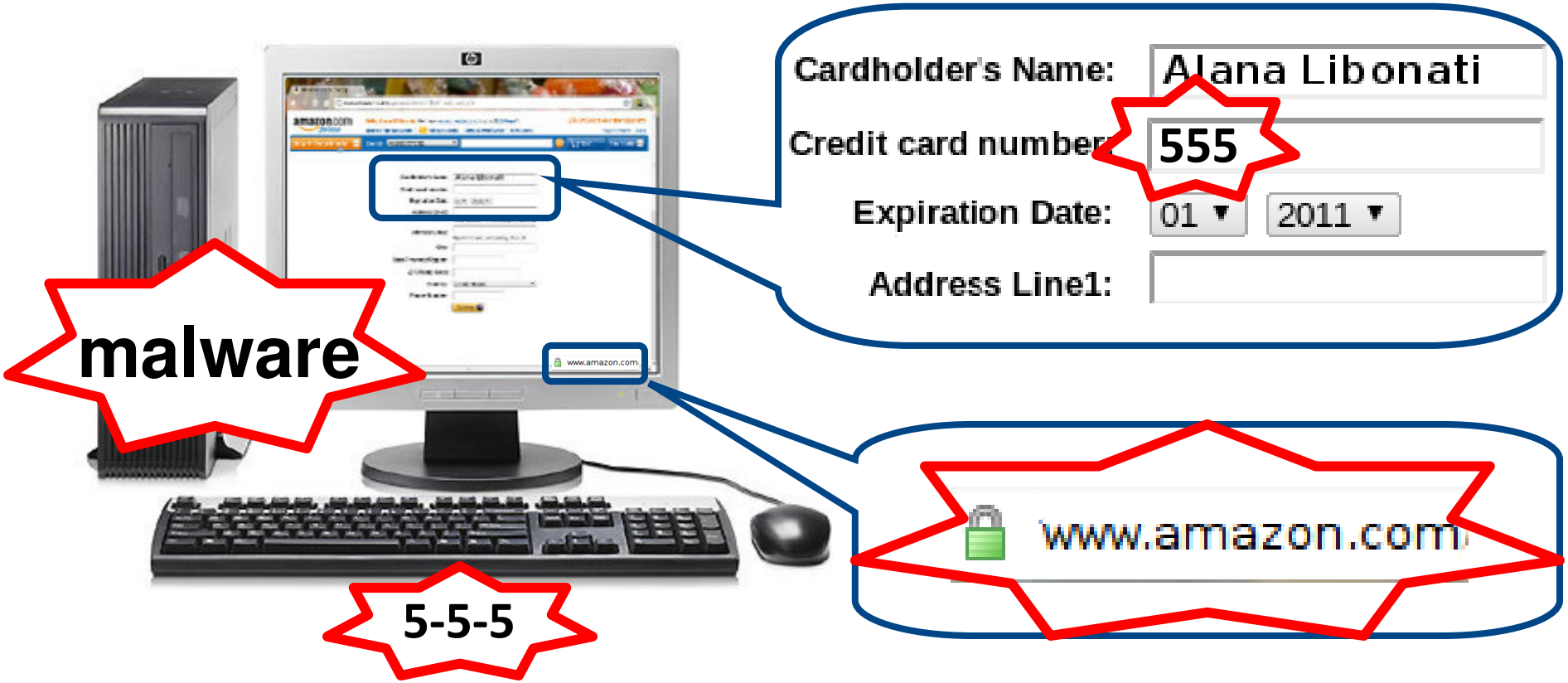
Carnegie Mellon University[2]

February 16, 2011

Carnegie Mellon CyLab CONFIDENCE FOR A NETWORKED WORLD

Motivation

Consider a user providing sensitive information via a web form



Threat Model

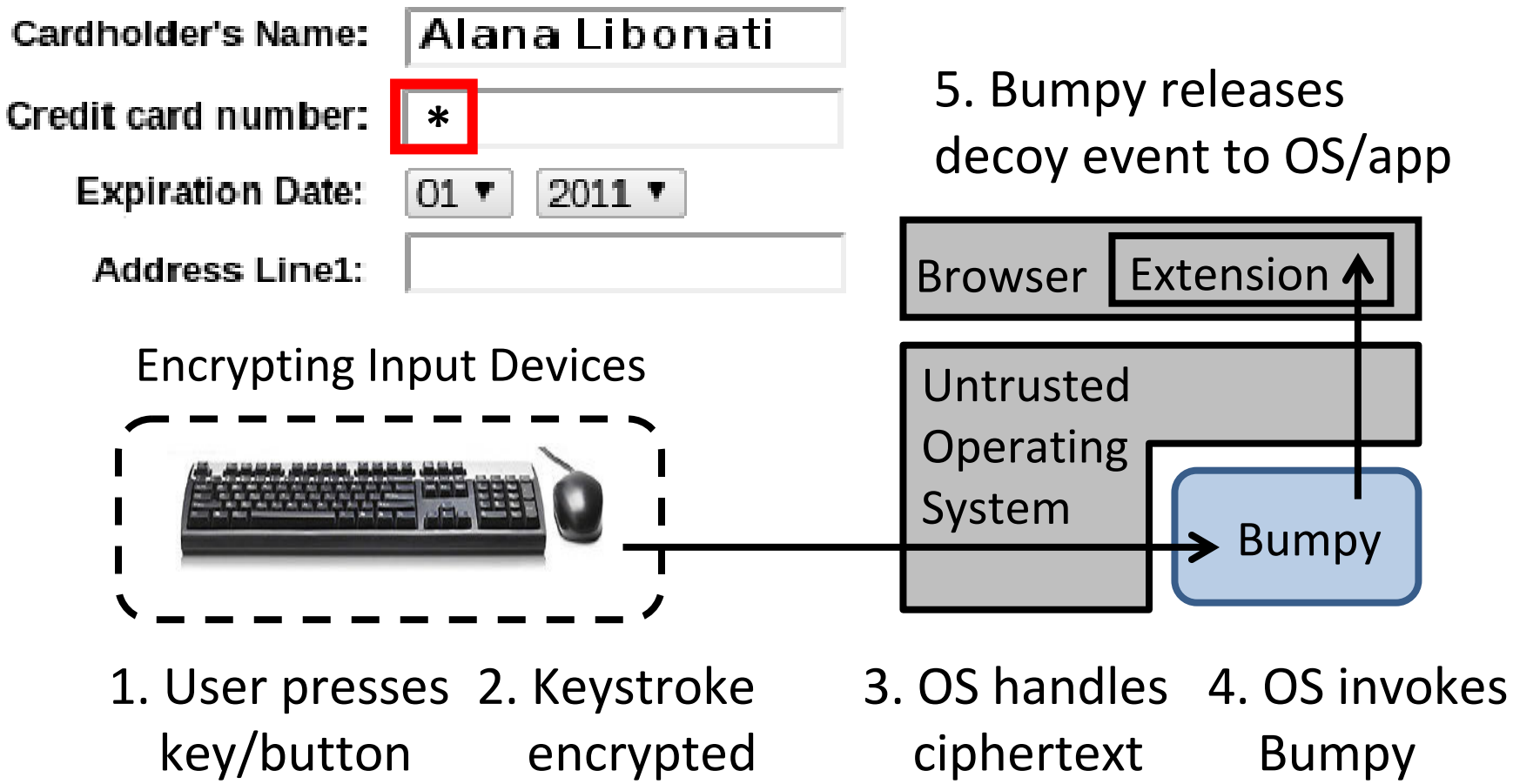
Operating system (and applications) compromised

- Host-based malware can capture user input
- On-screen security indicators cannot be trusted

Destination website uncompromised

Bumpy [McCune et al. NDSS 09]

Protects user input from malware



Bumpy [McCune et al. NDSS 09]

How it's used:

- User decides which fields are sensitive by preceding them with a Secure Attention Sequence (SAS)

- User confirms where input will be sent using a physically separate device (Trusted Monitor)
    - External devices uncompromised in our threat model

How Usable Is Bumpy?

Users must be extra diligent:

- Remember to precede sensitive input with a SAS
- Remember to verify destination on Trusted Monitor (TM)
- React to unexpected results
- Mistrust their own computers!

Our goals:

- Quantify the usability
- Try to improve it

Our Study

Simulated 4 different Bumpy interfaces:

- Varied method of SAS entry
- Varied the way users interacted with TM

Tested usability in:

- Benign circumstances (success rate, duration)
- Simulated malware attacks (password characters leaked)

Provides broader insights:

- Designing secure interfaces
- Training effectiveness

Design 1 of 4: Original [McCune et al. NDSS 09]

Step 1:

The user prefixes her input with a secure attention sequence (SAS)

Design 1 of 4: Original [McCune et al. NDSS 09]

Cardholder's Name: Alana Libonati

Credit card number: @@

Expiration Date: 01 2011

Address Line1:

Street address, P.O. box, company name, c/o

Address Line2:

Apartment, suite, unit, building, floor, etc.

City:

State/Province/Region:

ZIP/Postal Code:

Country: United States

Phone Number:

Continue

Step 2:

The user verifies the destination for her input on the Trusted Monitor

Bumpy

https://www.amazon.com

Design 1 of 4: Original [McCune et al. NDSS 09]

Step 3:

The user types her input

Design 1 of 4: Original [McCune et al. NDSS 09]

Cardholder's Name: Alana Libonati

Credit card number: @@**********

Expiration Date: 01 2011

Address Line1: @@**********

Street address, P.O. box, company name, c/o

Address Line2: @@*****

Apartment, suite, unit, building, floor, etc.

City: Carrboro

State/Province/Region: NC

ZIP/Postal Code: 27510

Country: United States

Phone Number: 919-442-1234

Continue

Design 2 of 4: Graphical

- Slight modification to Original
- Entry of SAS replaced by mouse clicking

Design 2 of 4: Graphical

Cardholder's Name: Alana Libonati

Credit card number:

Expiration Date: 01 2011

Address Line1:

Street address, P.O. box, company name, c/o

Address Line2:

Apartment, suite, unit, building, floor, etc.

City:

State/Province/Region:

ZIP/Postal Code:

Country: United States

Phone Number:

Continue

Step 1:

The user clicks inside a field to gain focus

Design 2 of 4: Graphical

Cardholder's Name: Alana Libonati

Credit card number:

Expiration Date: 01 2011

Address Line1:

Street address, P.O. box, company name, c/o

Address Line2:

Apartment, suite, unit, building, floor, etc.

City:

State/Province/Region:

ZIP/Postal Code:

Country: United States

Phone Number:

Continue

Step 2:

The user double-clicks within the field toggle its sensitivity

Design 2 of 4: Graphical

Cardholder's Name: Alana Libonati

Credit card number:

Expiration Date: 01 2011

Address Line1:

Street address, P.O. box, company name, c/o

Address Line2:

Apartment, suite, unit, building, floor, etc.

City:

State/Province/Region:

ZIP/Postal Code:

Country: United States

Phone Number:

Continue

Step 3:

The user verifies the destination for her input on the Trusted Monitor

Bumpy

https://www.amazon.com

Design 2 of 4: Graphical

Cardholder's Name: Alana Libonati

Credit card number: **********

Expiration Date: 01 2011

Address Line1:

Street address, P.O. box, company name, c/o

Address Line2:

Apartment, suite, unit, building, floor, etc.

City:

State/Province/Region:

ZIP/Postal Code:

Country: United States

Phone Number:

Continue

Step 4:

The user types her input

Design 2 of 4: Graphical

Cardholder's Name: Alana Libonati

Credit card number: **********

Expiration Date: 01 ▾ 2011 ▾

Address Line1: **********

Street address, P.O. box, company name, c/o

Address Line2: *****

Apartment, suite, unit, building, floor, etc.

City: Carrboro

State/Province/Region: NC

ZIP/Postal Code: 27510

Country: United States ▾

Phone Number: 919-442-1234

Continue

Design 3 of 4: NoTM

- User proactively instructs Bumpy where input should be sent
- No Trusted Monitor
- Favorite of one author
  - Users tend to ignore passive security indicators
  - Similar to direct navigation

Design 3 of 4: NoTM

Cardholder's Name: Alana Libonati

Credit card number:

Expiration Date: 01 2011

Address Line1:

Street address, P.O. box, company name, c/o

Address Line2:

Apartment, suite, unit, building, floor, etc.

City:

State/Province/Region:

ZIP/Postal Code:

Country: United States

Phone Number:

Continue

Input is prefixed by a user defined SAS

@ama@

Design 4 of 4: Challenge

- TM displays a random challenge that must be typed
- Requires the user to look at the TM

Design 4 of 4: Challenge

Cardholder's Name: Alana Libonati

Credit card number: @@

Expiration Date: 01 2011

Address Line1:

Street address, P.O. box, company name, c/o

Address Line2:

Apartment, suite, unit, building, floor, etc.

City:

State/Province/Region:

ZIP/Postal Code:

Country: United States

Phone Number:

Continue

Step 1:

The user prefixes her input with a SAS

Design 4 of 4: Challenge

Cardholder's Name: Alana Libonati

Credit card number: @@

Expiration Date: 01 2011

Address Line1:

Street address, P.O. box, company name, c/o

Address Line2:

Apartment, suite, unit, building, floor, etc.

City:

State/Province/Region:

ZIP/Postal Code:

Country: United States

Phone Number:

Continue

Step 2:

The user verifies the destination and checks the random challenge displayed on the TM

Bumpy

https://www.amazon.com

Type the following: 73

Design 4 of 4: Challenge

Cardholder's Name: Alana Libonati

Credit card number: @@73

Expiration Date: 01 2011

Address Line1:

Street address, P.O. box, company name, c/o

Address Line2:

Apartment, suite, unit, building, floor, etc.

City:

State/Province/Region:

ZIP/Postal Code:

Country: United States

Phone Number:

Continue

Step 3:

The user enters the challenge, followed by her input

Design 4 of 4: Challenge

Cardholder's Name:	Alana Libonati
Credit card number:	@@73**********
Expiration Date:	01 ▾ 2011 ▾
Address Line1:	@@42**********
	Street address, P.O. box, company name, c/o
Address Line2:	@@58*****
	Apartment, suite, unit, building, floor, etc.
City:	Carrboro
State/Province/Region:	NC
ZIP/Postal Code:	27510
Country:	United States ▾
Phone Number:	919-442-1234

Continue

Next: Study Methodology

- Bumpy
- User experience
- Study methodology

User Interface Simulation

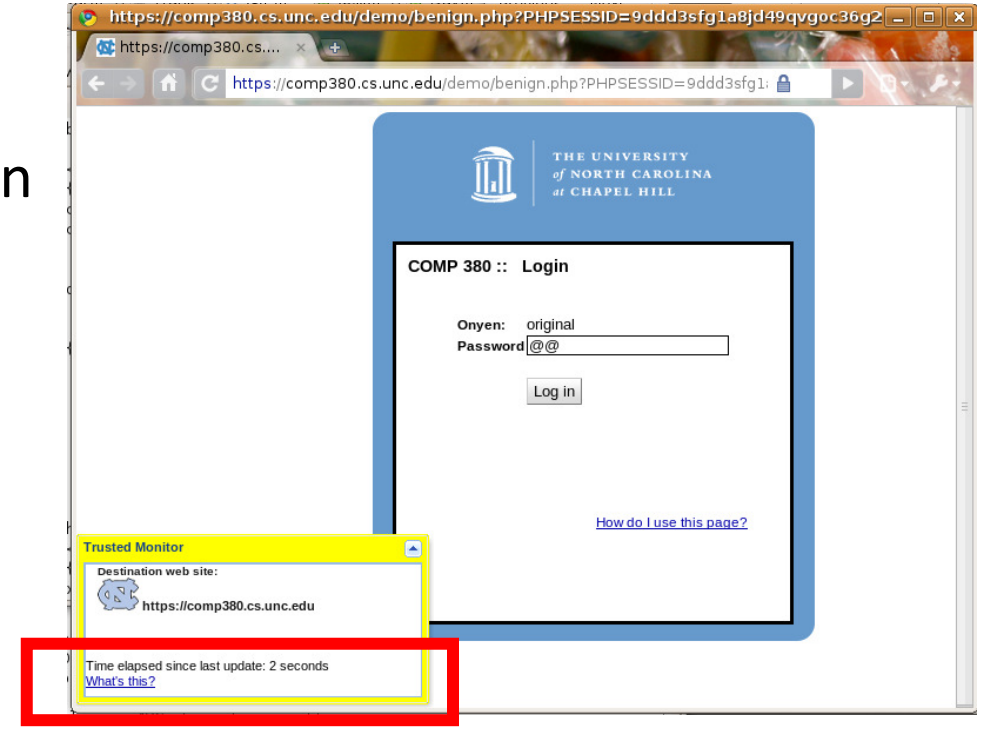
Study participants used one of the four Bumpy designs to protect password entries to a course web page

Challenge:

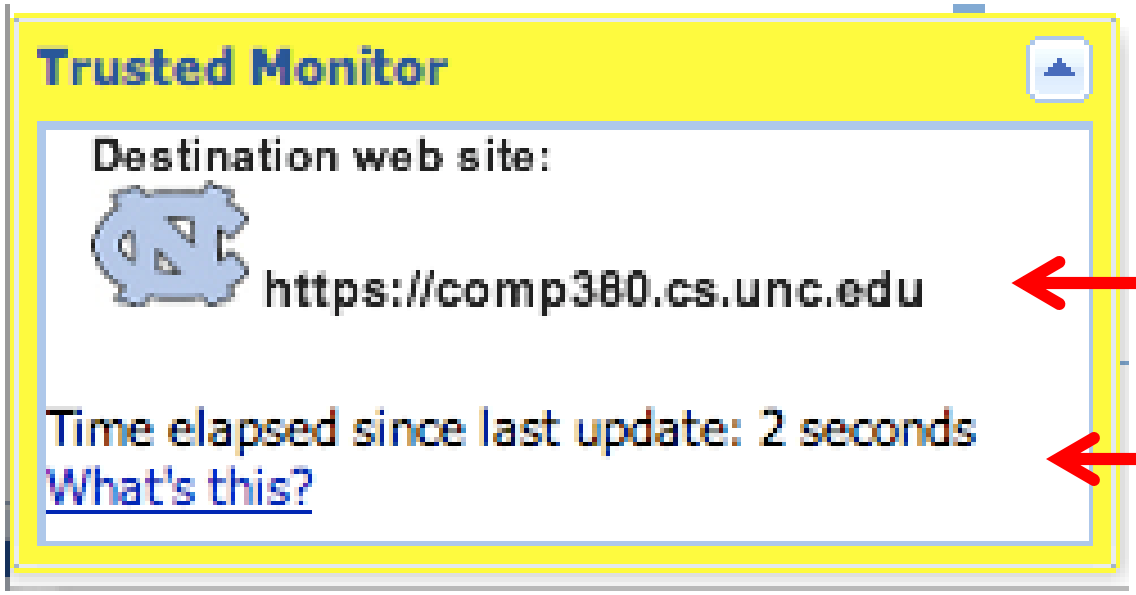
- Unable to provide users with a physical Trusted Monitor

Solution:

- Entirely web based simulation



User Interface Simulation



Domain name, favicon

Elapsed time indicator

Other features:

- Audible beep
- Visual color flash

Logging

- Collected time-stamped information about:
  - Mouse clicks
  - Keystrokes
  - Focus events
- Necessary for ordering events, computing login duration
- Complete record of all user activity

Participant Enrollment

- Participants were 85 out of 136 students enrolled in *COMP 380: Computers and Society*
  - 28 majors represented
- Offered possible cash award (up to $150 per user)
  - Reduced when password characters were leaked
  - Increased when they logged in frequently

Participant Enrollment

- Students were assigned to one of the four Bumpy designs or a Control design

- Breakdown of users per design:

Original	17
Graphical	16
NoTM	17
Challenge	19
Control	16

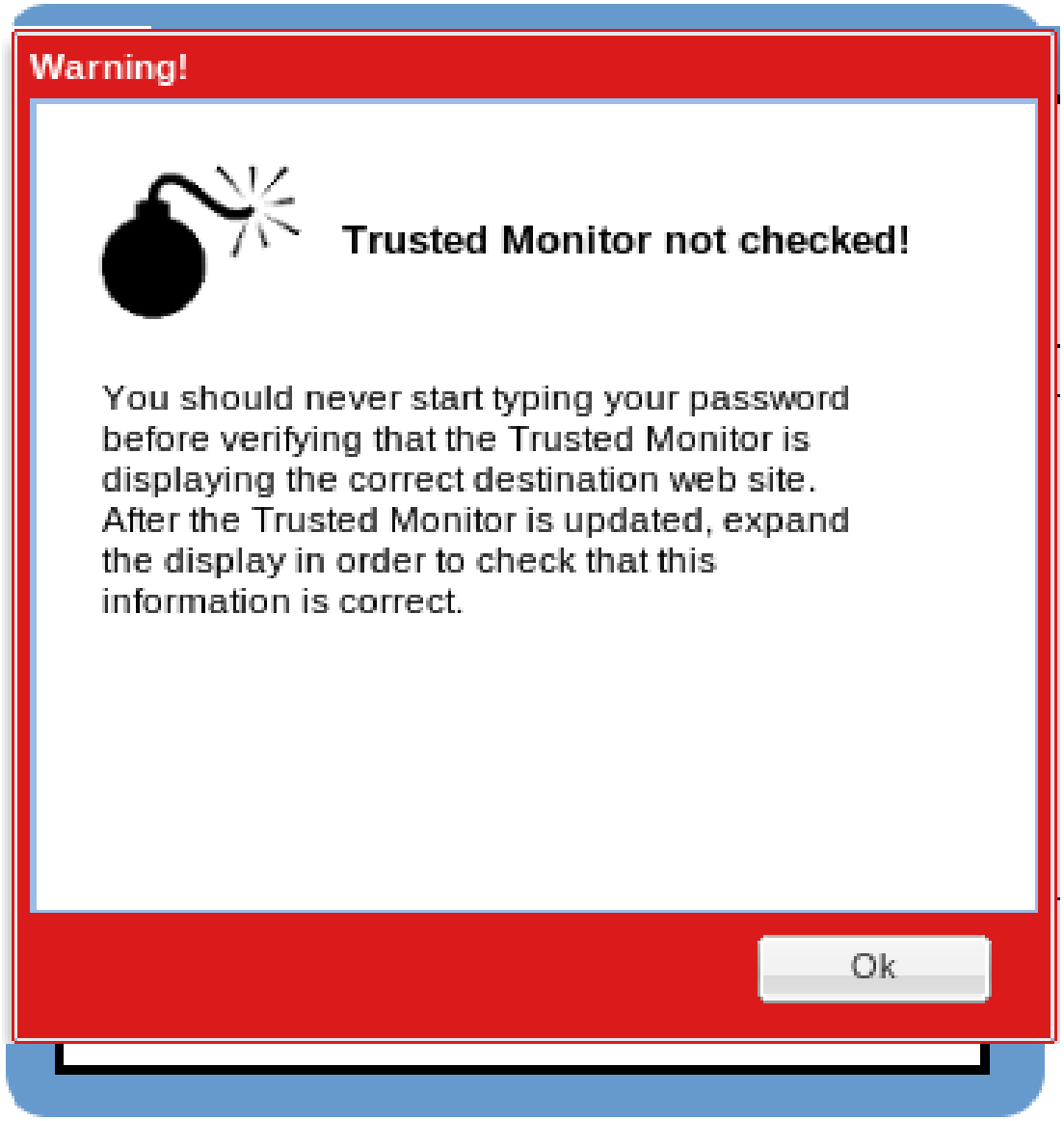
Experiment Timeline

- Experiment was conducted in four phases:

- Walkthrough video and help page:
  - Accessible throughout all four phases
  - Explained login process (for benign logins)
  - Suggested reloading the page if things were “abnormal”

Initial | Benign | Attack | Attack-and-Warn

- Training phase
- Automated instructions
- No simulated attacks
- Duration: 15 days

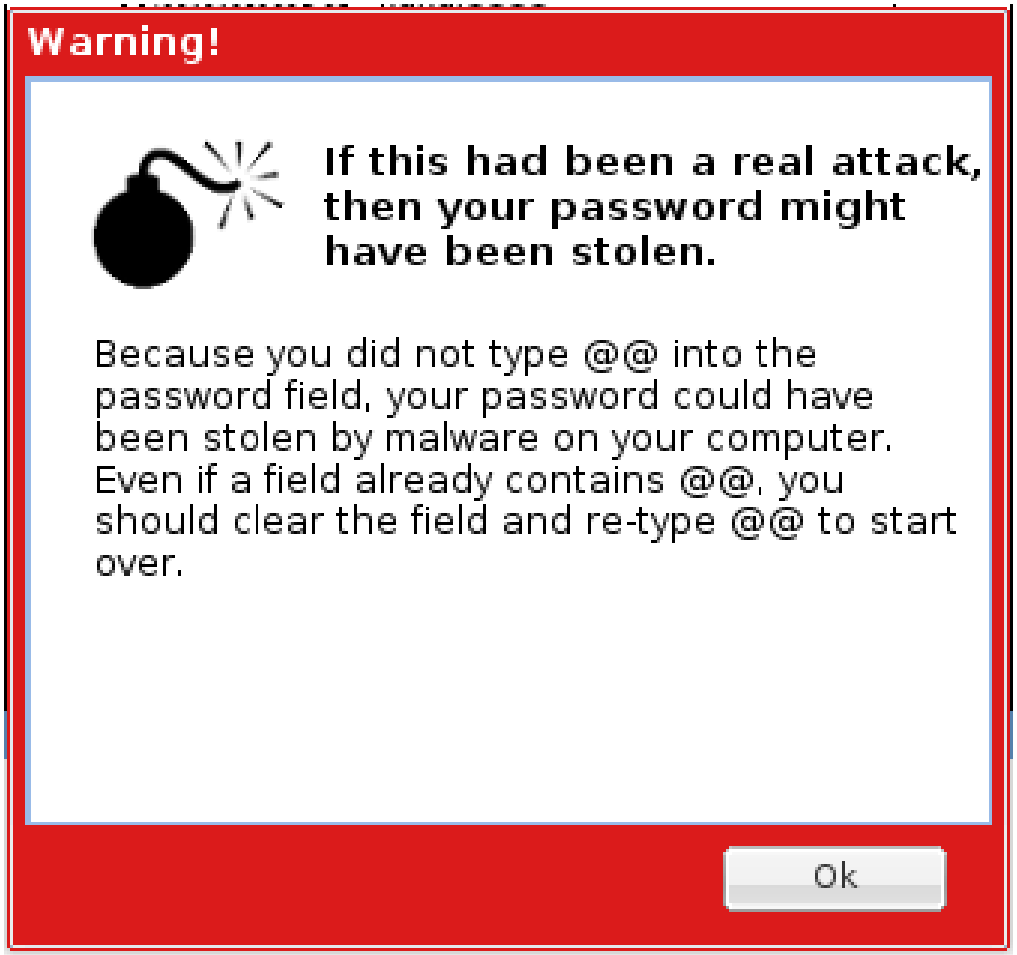


- Gives a baseline login success rate and duration
- Automated instructions disabled
- No simulated attacks
- Duration: 28 days

- Used to compute password leakage statistics
- Simulated a malware attack with probability .5
- Duration: 26 days

Initial → Benign → Attack → Attack-and-Warn

- Used to evaluate the effectiveness of warnings as a form of training
- Simulated a malware attack with probability .5
- Users were warned after "improper" login attempts
- Duration: 38 days



Attacks

Threat Model

- Operating system (and applications) compromised
- Trusted Monitor and destination website uncompromised

- Active attacks: Feigned-Fail, Wrong-Dest, SAS-Present
- Always subject to passive attack

Active Attack 1 of 3: Feigned-Fail

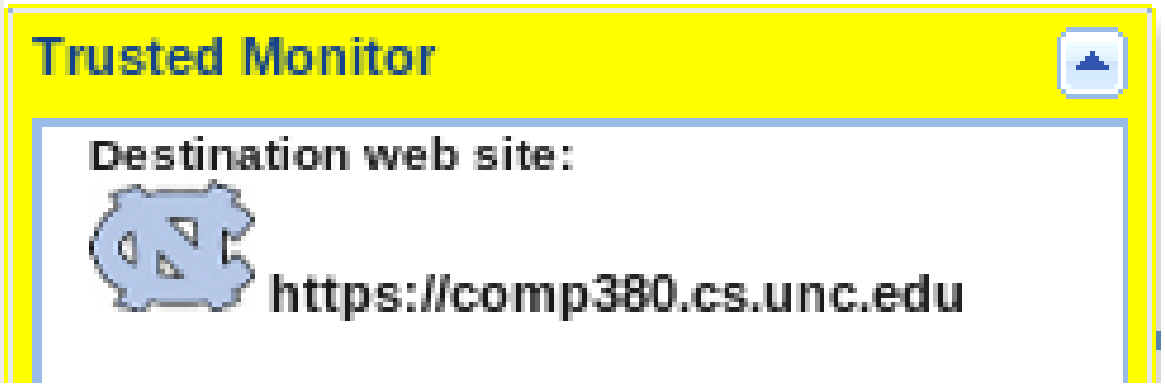
- Malware that interferes with Bumpy's operation
  - TM not updating (in designs that use a TM)
  - Per-site SAS not recognized (in the NoTM design)
- Designed to frustrate users

Active Attack 2 of 3: Wrong-Dest

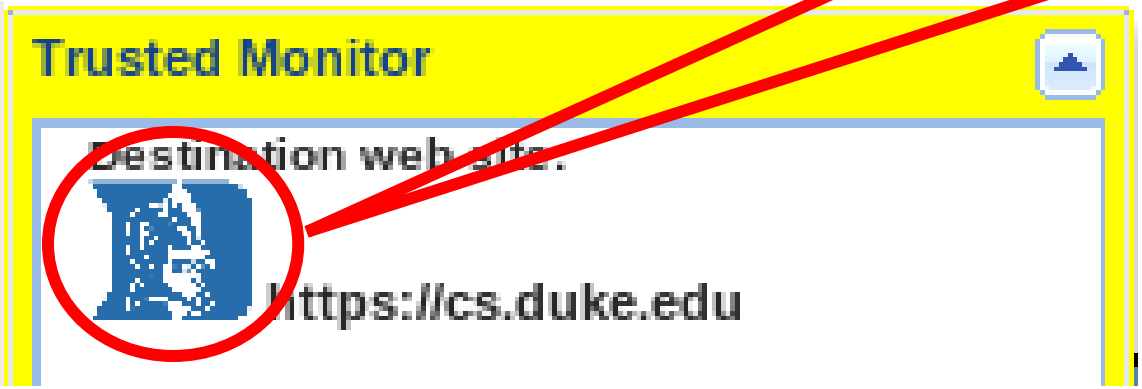
- Wrong destination shown on Trusted Monitor
- Represents malware trying to redirect input

Active Attack 2 of 3: Wrong-Dest

User should see:

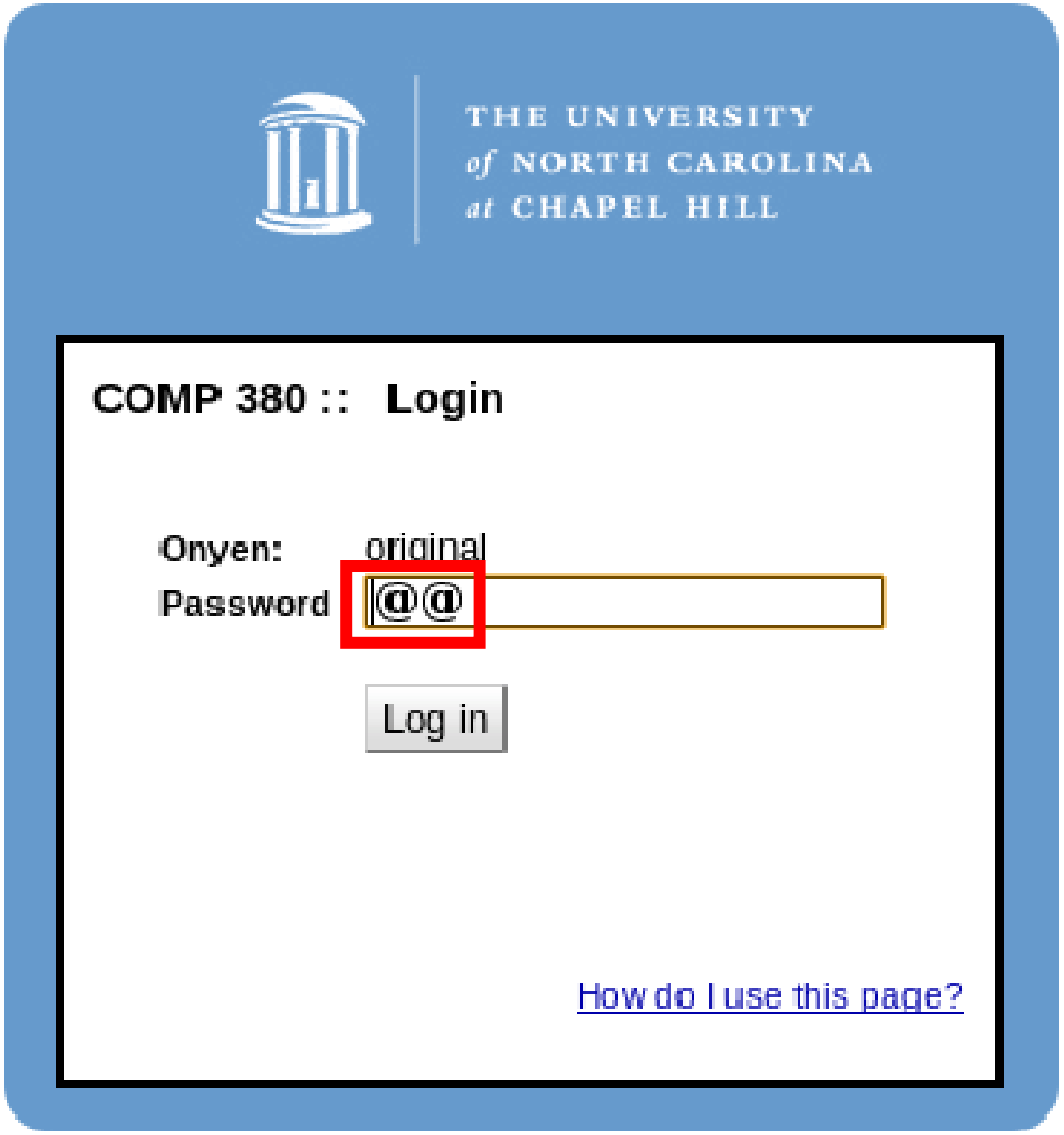


User instead sees:



Active Attack 3 of 3: SAS-Present

- Page loads with SAS already filled in
- Designed to trick users into not using Bumpy

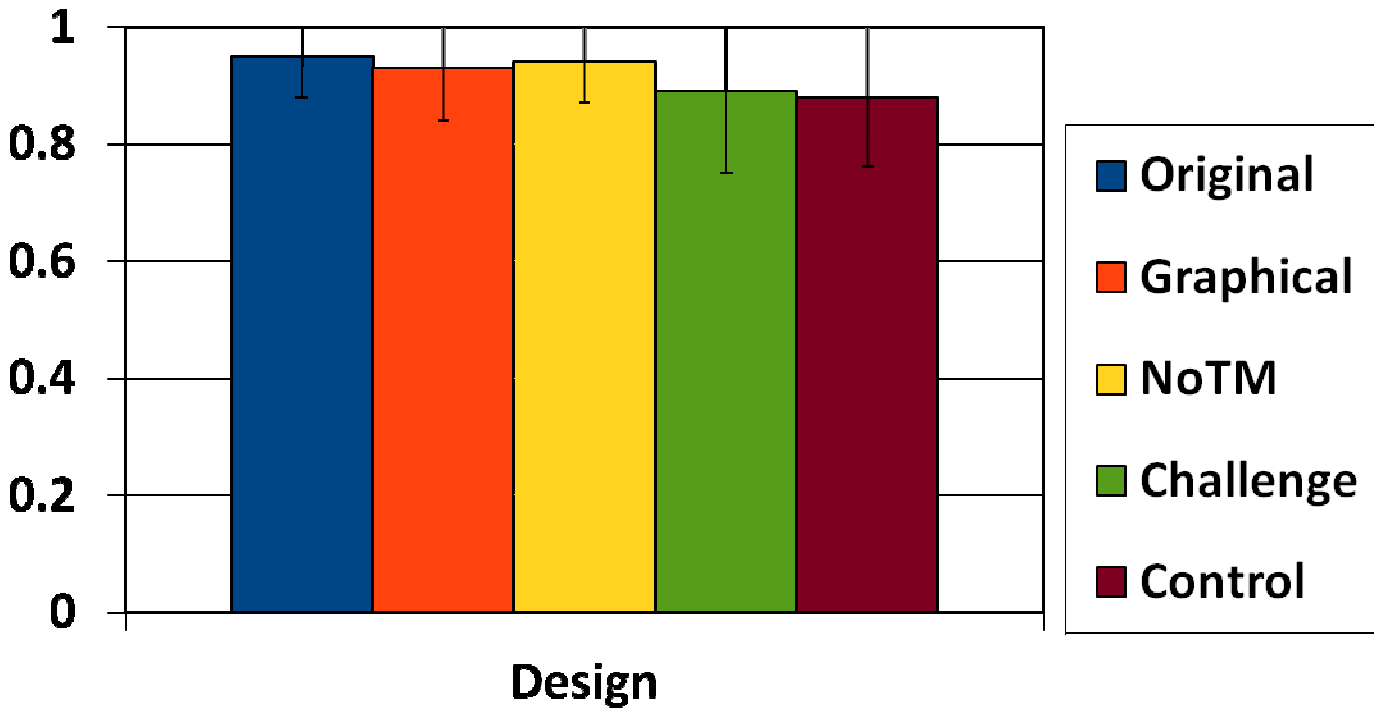


Results

1. Login success rate, duration
2. Avg/max fraction of password leaked
3. Effectiveness of warnings

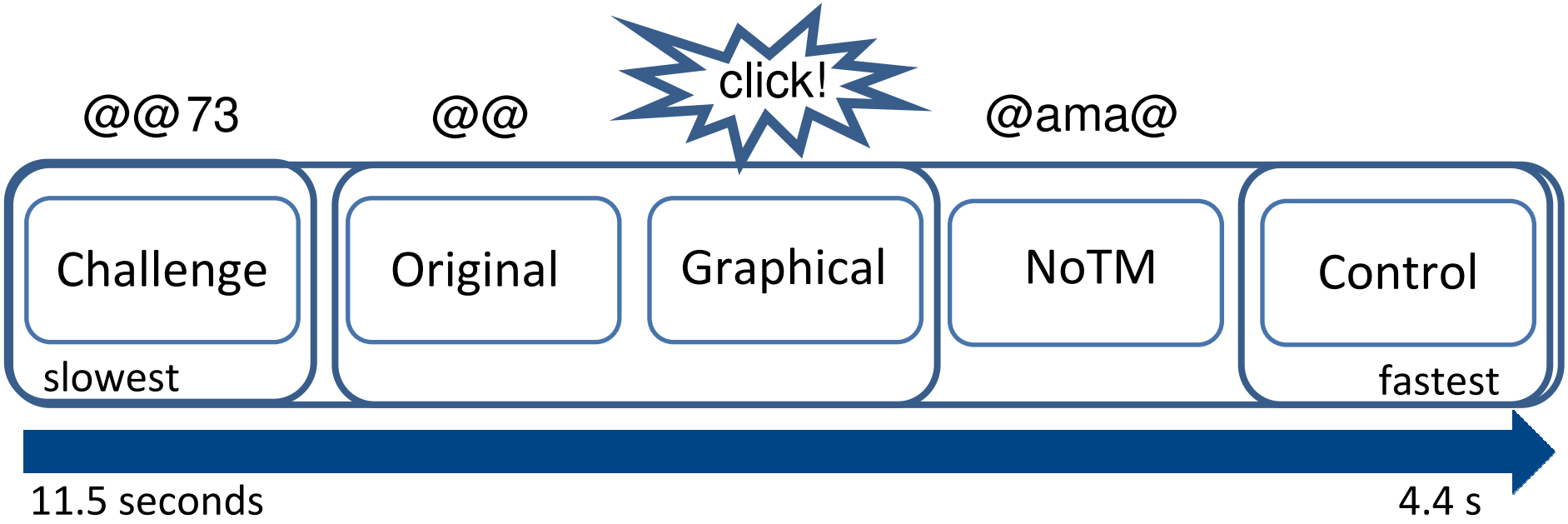
Benign Phase: Login Success Rate

$$\text{success rate} = \frac{\text{successful logins}}{\text{all attempted logins}}$$



Analysis of Variance (ANOVA) revealed no significant differences between designs

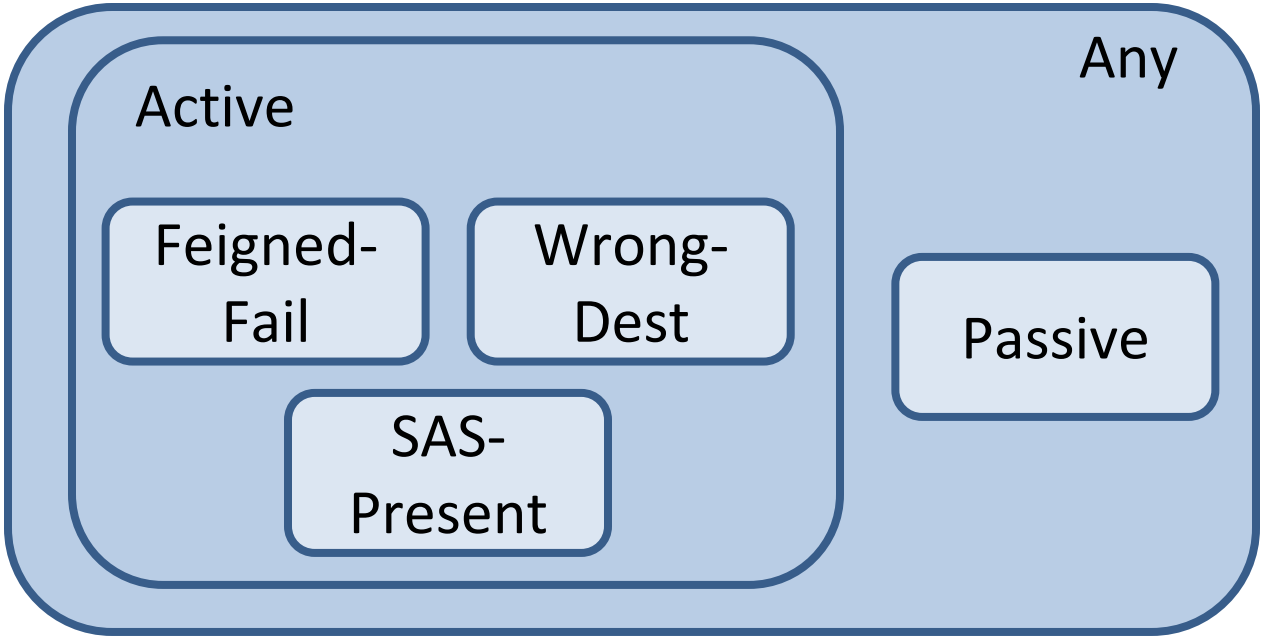
Benign Phase: Login Time



- Control was significantly faster than designs using a TM
  - Opening and inspecting the TM takes time
- Challenge was significantly slower than rest of the designs
  - Extra diligence required to copy value from TM

Attack Phase: Password Leakage

Considered following categories of attacks:



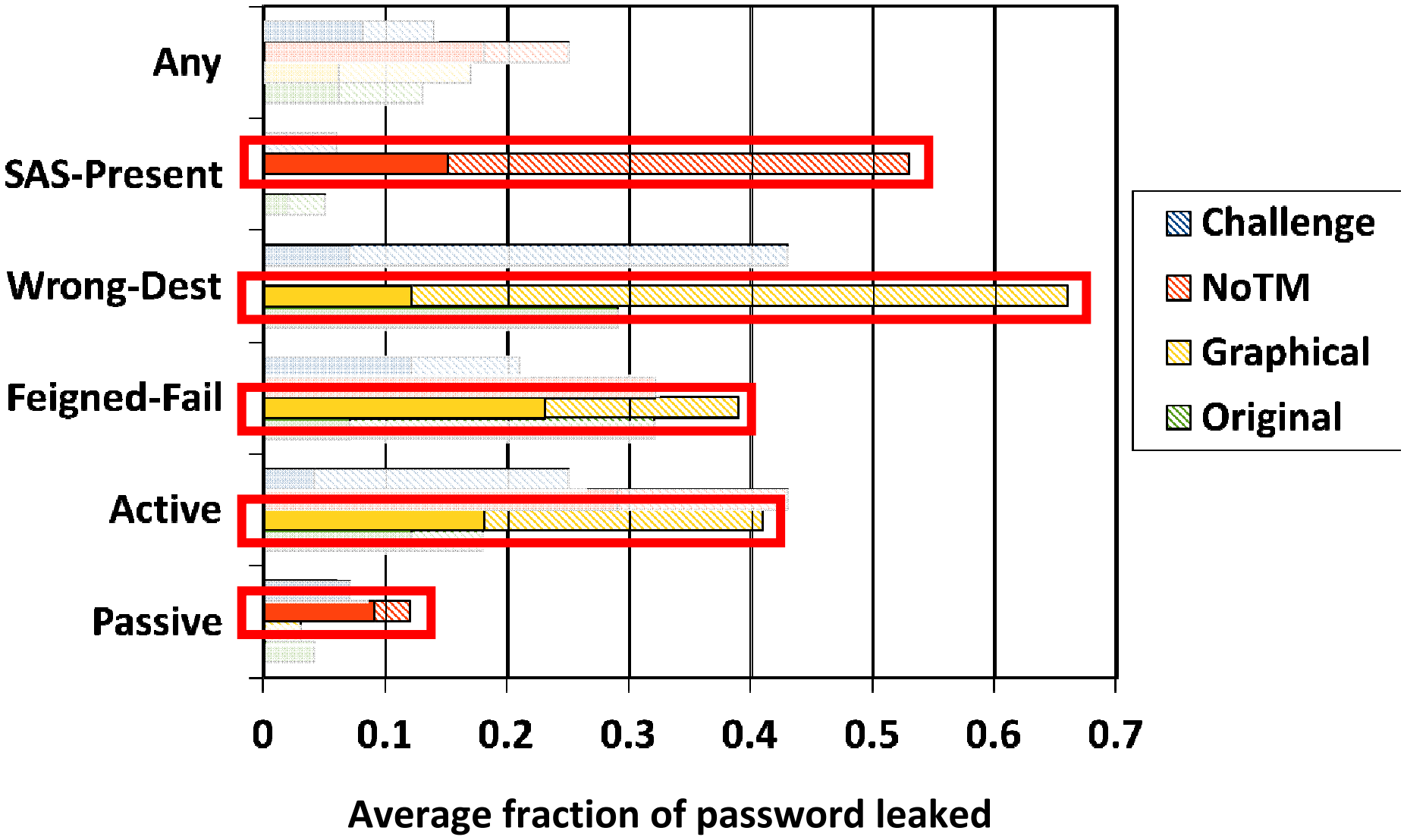
For each category, calculated the average and maximum fraction of password leaked

Attack Phase: Password Leakage

SAS-Present attack:

- NoTM had significantly greater leakage than Original and Challenge against SAS-Present attack
  - Original and Challenge provide feedback user expects to see before entering input

Attack-and-Warn Phase: Training Effectiveness



Conclusions: Design-Specific

NoTM design

Fastest	Users require more training
Attractive for deployment	

Challenge design

Low password leakage	Slowest

Graphical design

	No strong benefits

Conclusions: Broader Insights

Results indicate that:

- Users readily adapt to employing secure attention sequences
- Challenge-response security indicators better than passive ones

Interesting open questions:

- Is repeating a task following a mistake warranted?
- Can a login system offer both speed and security?